UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of Information associated with the Discord, Inc. Accounts: a. hardline2042@outlook.com, Vanhorn#1518, 1049848180231127111; b. hardline2077@outlook.com, Cassidy Harding#5154, 1038972467848421376; c. Deleted User 4dc07823#7222, 850446314859921451 That is Stored at the Premises Controlled by Discord, Inc., 444 De Haro St., Suite 200, San Francisco, CA 94107	**UNDER SEAL** Case No 2:24sw 48

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property: **See Attachment A-2.**

Located in the Northern District of California, and elsewhere, there is now concealed:

See Attachment B-2.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt and Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts: **See Affidavit**.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S .C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Applicant's signature

Victoria Liu
Special Assistant United States Attorney

Lindsey Santos, Special Agent, NCIS
Printed name and title

Sworn to before me and signed in my presence.

Date: March 20, 2024

Judge's signature

City and state: Norfolk, VA

Honorable Robert J. Krask

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT COURT OF VIRGINIA
Norfolk Division

IN THE MATTER OF THE SEARCH OF:	)	**UNDER SEAL**
(1) INFORMATION ASSOCIATED WITH THE MICROSOFT CORPORATION USA ACCOUNTS: a. hardline2042@outlook.com b. hardline2077@outlook.com **That is Stored at the Premises Controlled by Microsoft Corporation USA, 1 Microsoft Way, Redmond, WA 98052.**	)	**Case No. 2:24sw 47**
(2) INFORMATION ASSOCIATED WITH THE DISCORD, INC. ACCOUNTS: a. Email Address: hardline2042@outlook.com Screen/User Name: Vanhorn#1518 ESP User ID: 1049848180231127111 b. Email Address: hardline2077@outlook.com Screen/User Name: Cassidy Harding#5154 ESP User ID: 1038972467848421376 c. Screen/User Name: Deleted User 4dc07823#7222 ESP User ID: 850446314859921451 **That is Stored at the Premises Controlled by Discord Inc., 444 De Haro St., Suite 200, San Francisco, CA 94107.**	)	**Case No. 2:24sw 48**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Lindsey Santos, being first duly sworn state:

1. I am presently employed as a Special Agent with the United States Naval Criminal Investigative Service (NCIS), where I have worked since August 2022. In that capacity, my duties including investigating federal criminal offenses in the Eastern District of Virginia, to include

Internet Crimes Against Children (ICAC), namely investigating activities relating to material constituting or containing child pornography.

2. During my tenure as a Special Agent, I have completed approximately 500 hours of instruction at the Federal Law Enforcement Training Center in Glynco, Georgia (FLETC). While at FLETC, I completed blocks of instruction and labs that have enabled me to identify potential sources of electronic evidence, including but not limited to computers, cell phones, and other digital storage media and to preserve and exploit such evidence.

3. Prior to my tenure as a Special Agent, I was employed by the Norfolk Police Department from July 2015 to August 2022 and was assigned to the Vice and Narcotics Division from July 2018 to August 2022. During my assignment to the Vice and Narcotics Division, I was tasked with investigating Human Trafficking, Narcotics, and Child Exploitation, both as an investigator and an undercover officer.

4. I have had training in both Child Pornography Detection and Investigations and am a member of the Internet Crimes against Children (ICAC) Task Force. Further, I received advanced training in Human Trafficking investigations and am a member of the Department of Homeland Security, Human Trafficking Task Force as a Task Force Officer since September 2020.

5. I have conducted and completed well over 100 criminal investigations at the local, state, and federal level, which resulted in over 100 convictions of crimes ranging from larceny to that of possession of a controlled substance as well as Human Trafficking and Child exploitation. Moreover, I have conducted and participated in over 50 search warrants, to include that of premises as well as electronic devices, cloud computing storage, and persons, as well as over 400 interviews of suspects, witnesses, and victims.

6. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

7. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require Discord Inc. and Microsoft Corporation USA (the "Providers") to disclose to the government records and other information in its possession pertaining to the subscribers or customer(s) associated with the accounts, including the contents of communications. The information to be searched and seized is described in the following paragraphs and in Attachments A-1 and A-2, further described in Attachments B-1 and B-2.

8. This affidavit is being submitted in support of an application for a search warrant for the information and content associated with the **SUBJECT ACCOUNTS 1-5**, specifically described as:

A. Microsoft outlook e-mail accounts associated with the following identifiers:

a. **Email: hardline2042@outlook.com ("Subject Account 1")**
b. **Email: hardline2077@outlook.com ("Subject Account 2")**

from April 1, 2022, to present, which are stored at the premises owned, maintained, controlled, or operated by Microsoft Corporation USA, 1 Microsoft Way, Redmond, WA 98052, as described in Attachment A-1.

B. Discord, Inc. accounts associated with the following identifiers:

a. **Email Address: hardline2042@outlook.com**
Screen/User Name: Vanhorn#1518
ESP User ID: 1049848180231127111 ("Subject Account 3")

b. **Email Address: hardline2077@outlook.com**
Screen/User Name: Cassidy Harding#5154

ESP User ID: 1038972467848421376 ("Subject Account 4")

c. **Screen/User Name: Deleted User 4dc07823#7222**
ESP User ID: 850446314859921451 ("Subject Account 5")

from April 1, 2022, to present, which are stored at the premises owned, maintained, controlled, or operated Discord, Inc., a company headquartered at 444 De Haro St, Suite 200, San Francisco, CA 94107, as described in Attachment A-2.

9. Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) (the "Target Offenses") have been violated by the user(s) of the **SUBJECT ACCOUNTS**. There is also probable cause to search the information in Attachments A-1 and A-2 for evidence of these crimes, as described in Attachments B-1 and B-2.

JURISIDICTION

10. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the court is "a district court of the United States… that has jurisdiction over the offense being investigated." 18 U.S.C § 2711(3)(A)(i). This investigation involves an offense within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below.

PERTINENT FEDERAL CRIMINAL STATUTES

11. Title 18, United States Code, § 2252(a)(2) makes it a crime to knowingly receive or distribute, using any means or facility of interstate or foreign commerce or that has been mailed, shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed, shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate

or foreign commerce or in or affecting interstate or foreign commerce or through the mails, any visual depiction of minors engaging in sexually explicit conduct.

12. Title 18, United States Code, § 2252(a)(4)(B) makes it a crime to knowingly possess or access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

LEGAL AUTHORITY

13. The legal authority for this search warrant application regarding electronic mail accounts is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C. § 2703(b) provides in relevant part as follows:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
>
> (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

14. The government may also obtain records relating to email communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

15. 18 U.S.C. § 2703(c)(1)(A), provides, in part, that the Government may also obtain non-content records and other information pertaining to a customer or subscriber of an electronic communication service or remote computing service by means of search warrant.

16. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

DEFINITIONS

17. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

18. "Child Erotica" as used herein, refers to materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. Such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

19. "Minor" and "sexually explicit conduct" are defined in 18 U.S.C. §§ 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

a. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
b. Bestiality;
c. Masturbation;
d. Sadistic or masochistic abuse; or
e. Lascivious exhibition of the genitals or pubic area of any person.

20. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. 18 U.S.C. § 1030(e)(1).

21. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related

communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

22. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

23. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

24. "Electronic Communication Service" refers to any service, which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

25. "Electronic communication service provider" (ECSP) means (a) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934; (b) a provider of electronic communication service, (c) a provider of a remote computing service, (d) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are

stored; or (e) an officer, employee, or agent of an entity described in subparagraph (a), (b), (c), or (d).

26. Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

27. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

28. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

29. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

30. "Internet Protocol Address" (IP Address), as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP Addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the

Internet. IP Addresses might also be "static," if an ISP assigns a user's computer a particular IP Address that is used each time the computer accesses the Internet.

31. "Remote Computing Service" as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

32. Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

33. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log-on/log-off times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

34. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. graphic records or representations;
b. photographs;
c. pictures;

d. images, and
e. aural records or representations.

35. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

36. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

37. Based upon the information officially supplied to me by other law enforcement officers, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to

the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases

where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC)

38. The National Center for Missing and Exploited Children (NCMEC) is a non-profit organization that provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its Congressional authorization (former 42 USC § 5773, now 34 USC § 11293), the NCMEC is statutorily obliged to operate the official national clearinghouse for information about missing and exploited children, to help law enforcement locate and recover missing and exploited children, to "provide forensic technical assistance ... to law enforcement" to help identify victims of child exploitation, to track and identify patterns of attempted child abductions for law enforcement purposes, to "provide training ... to law enforcement agencies in identifying and locating non-

compliant sex offenders," and to operate the CyberTipline as a means of combating Internet child sexual exploitation.

39. The NCMEC and the NCMEC alone is statutorily obliged to maintain an electronic tipline for Electronic Communication Service Providers (ECSPs) to use to report possible Internet child sexual exploitation violations to the government. CyberTips are investigative leads generated by the NCMEC. The NCMEC is obliged to forward every single report it receives to federal law enforcement agencies, and it may make its reports available to state and local law enforcement as well. In aid of its tipline functions, the NCMEC is statutorily authorized to receive contraband (child pornography) knowingly and to review its contents intentionally.

40. In accordance with 18 U.S.C. § 2258A, if an ECSP becomes aware of facts or circumstances indicating there may be a violation of federal child pornography laws, the ECSP submits a CyberTipline report to the NCMEC. While ECSPs will report the presence of any suspected child pornography they find to the NCMEC, they do not conduct an exhaustive search of a user's account or cloud storage, but typically use some automated method for locating images of suspected child pornography. This may include the use of automated technologies that compare the hash values of images contained in the user's account to the hash values of images of child pornography.

41. When the NCMEC receives a CyberTipline report from an ECSP related to the sexual exploitation of children, NCMEC analysts conduct preliminary research to determine the possible location of the incident, and then forward the information to the appropriate Internet Crimes Against Children (ICAC) task force or the appropriate law enforcement agency for follow-up. In CyberTipline reports in which the ECSP does not view the image but rather relies on an

automated method to determine the contents, NCMEC does not look at the actual images of alleged child pornography; rather NCMEC analysts leave it up to the appropriate law enforcement agency to determine whether the images constitute child pornography.

TECHNICAL BACKGROUND ON MICROSOFT CORPORATION

42. Based on my training and experience, and publicly available information, I have learned that Microsoft Provides a variety of online services, including email (Outlook), online file storage (including Microsoft OneDrive), XBOX Gaming Services, and video calling (Skype), to the general public. Some services, such as Outlook email, online file storage, and messaging require the user to sign into the service using their Microsoft account. An individual can obtain a Microsoft account by registering with Microsoft, and the account identifier typically is in the form of an Outlook or Microsoft address. Other services, such as Skype, can be used while signed in to a Microsoft account, although some aspects of these services can be used even without being signed in to a Microsoft account.

43. Microsoft allows subscribers to obtain e-mail and other accounts at the domain name outlook.com, like the **SUBJECT ACCOUNTS** listed in Attachment A. Subscribers obtain an Outlook e-mail account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Outlook subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information.

44. In general, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Microsoft, and other ISPs have provided their users with larger storage capabilities associated with the user's e-mail account. Microsoft, and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.

45. When the subscriber sends an e-mail, it is initiated at the user's computer or mobile device, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft typically saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Microsoft server, the e-mail can remain on the system indefinitely.

46. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Microsoft but may not include all of these categories of data.

47. A Microsoft subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned

by Microsoft. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

48. Many subscribers to Microsoft do not store copies of the e-mails stored in their Microsoft account on their home computers. This is particularly true because they access their Microsoft account through the Internet, and thus it is not necessary to copy e-mails to a home computer to use the service. Moreover, an individual may not wish to maintain particular e-mails or files in their residence to ensure others with access to the computer cannot access the e-mails.

49. In my training and experience, generally, e-mail providers like Microsoft ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers (usually a mobile number) and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

50. The mobile number and alternate e-mail information provided to Microsoft, by the user are particularly useful in instances where a user needs to recover his/her account in the event of a lost password or account compromise. With these, Microsoft can send a "reset password" link to the alternate e-mail address, or an SMS message to the mobile number. Upon receiving the

"reset password" link to an SMS mobile number affiliated with that account, the user can then reset the password in order to continue to utilize that particular account. Because both a mobile device number and alternate e-mail address are used to recover access to an account, they both tend to be closely associated with the user of the account. It is important to note that though Microsoft attempts to validate the personal identifying information provided by subscribers, the validation requires additional voluntary input from users. As this additional input is voluntary, Microsoft is not always successful in validating a user's personal identifying information.

51. When creating an account at Microsoft, the user is provided the opportunity to create a display name and an associated "Profile." Microsoft allows a user to personalize their Profile by "adding an image that represents you." The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.

52. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Microsoft's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

53. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

54. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information such as name and address.

55. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

TECHNICAL BACKGROUND ON DISCORD, INC.

56. Based on my training and experience, and publicly available information, I have learned that Discord, Inc. operates as an electronic gaming company and user communications platform. Discord, Inc. is a proprietary freeware VoIP (Voice over Internet Protocol) application and digital distribution platform designed for video gaming communities that specializes in text, image, video and audio communication between users in a chat channel. Discord, Inc. runs on

Windows, MacOS, Android, iOS, Linux, and in web browsers. There are over 250 million unique users of the software worldwide.

57. Discord, Inc. allows subscribers to obtain a username by providing an e-mail address, like **SUBJECT ACCOUNTS 1 and 2** listed in Attachment A-1. Subscribers obtain a username and user identification number which is an eighteen (18) digit number unique to the user. During the registration process, Discord, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Discord, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved instant messages, emails, photos, videos, and documents) and information concerning subscribers and their use of Discord, Inc. services, such as account access information and account application information.

58. In general, once a user of Discord, Inc.'s application creates a username and account, the user can create a server and invite friends to join the invite link or join existing servers. Servers can be broken down into subcategories or "channels" where users can connect with each other by either chatting or calling. Users can also communicate through direct messages or private chats between one to ten users. Discord, Inc. allows users to communicate over voice, video, and text. Discord, Inc. was created for use by individuals playing video games to allow them to play and discuss games in private servers they have been invited into or created themselves. Discord, Inc. users can also send and receive images and videos.

59. Other information connected to a Discord, Inc. ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used. In addition, emails, messages, and attachments sent and received between users, web browser

activity, other account records and contact information can lead to the identification of instrumentalities of the crimes under investigation.

60. When creating an account at Discord, Inc., the user is provided the opportunity to create a display name and an associated "Profile." Discord, Inc. allows a user to personalize their Profile by "adding an image that represents you." The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.

61. In my training and experience, Discord, Inc. typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Discord, Inc.'s website), and other log files that reflect usage of the account. In addition, Discord, Inc. often has records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Discord, Inc. account. Discord, Inc. can be used to validate or refute data found on a user's devices and in some cases fill gaps in information otherwise no longer available. This may be important to establish actual user attribution to a device or devices.

62. According to Discord, Inc.'s privacy policy, it keeps device IDs and IP addresses related to users' activity. Discord, Inc. allows users to connect other social networking profiles to

a Discord, Inc. profile. Discord, Inc. keeps information from those linked social networking accounts. Discord also uses cookies to keep track of the user's computer and browser settings.

63. Therefore, Discord, Inc.'s servers are likely to contain stored electronic communications and information and a user's use of Discord, Inc.'s services.

PROBABLE CAUSE

64. On May 8, 2022, Discord, Inc. submitted CyberTip # 124312259 to the NCMEC regarding one of their users uploading child pornography to **SUBJECT ACCOUNT 5**.

65. Discord, Inc. included the file in question, which the Provider had viewed, and your affiant subsequently viewed and verified. The JPG image file depicted a pubescent female displaying her unclothed vagina. Included with the image was the IP address 216.54.92.122 (hereinafter, "the .122 IP address"), which was used to log into the account. Prior to legal process beign sent to Cox Communications, the .122 IP address was geolocated to Norfolk, VA. Subsequent to an Administrative Subpoena submitted by Virginia Beach Police Department, Cox Communications provided the .122 IP address was attributed to the American Warrior Network, Building R63, located on board Naval Station (NAVSTA) Norfolk at 1320 Gilbert St. Norfolk, VA 23511. Building R63 is a multi-unit residential barracks building, located on NAVSTA Norfolk. This building has overall wireless internet access with the ability for users to pay for and create accounts to access internet all throughout the building, with hundreds of Sailors accessing it at various times.

66. On May 11, 2022, Discord, Inc. submitted a second CyberTip # 124512539 to the NCMEC regarding one of their users uploading child pornography to **SUBEJCT ACCOUNT 5**.

67. Discord, Inc. included the file in question, which the Provider had viewed, and your affiant subsequently viewed and verified. The JPG image file depicted a pubescent female

displaying her unclothed vagina. Included with the image was the .122 IP address, which was used to log into the account.

68. On December 7, 2022, Discord, Inc. submitted CyberTip # 140953141 to the NCMEC regarding one of their users uploading child pornography to **SUBJECT ACCOUNT 4**.

69. Discord, Inc. included the file in question, which the Provider had viewed, and your affiant subsequently viewed and verified. This .JPG file was an image of a female infant vagina being held open by two fingers. Included with the image was the .122 IP address, which was used to upload the image.

70. Discord, Inc. supplied the following subscriber information, associated with the user of **SUBJECT ACCOUNT 4**:

> Email Address: **hardline2077@outlook.com** (Verified)
> Screen/User Name: Cassidy Harding#5154
> ESP User ID: 1038972467848421376
> IP Address: **216.54.92.122** (Upload) 12-06-2022 22:06:50 UTC

71. Therefore, based on this subscriber information, your affiant learned that **SUBJECT ACCOUNT 2** was a verified e-mail address associated with **SUBJECT ACCOUNT 4**, and the .122 IP address was used to upload a file to **SUBJECT ACCOUNT 4** on December 6, 2022.

72. On December 13, 2022, Discord, Inc. submitted CyberTip # 141478559 to the NCMEC regarding one of their users uploading child pornography to **SUBJECT ACCOUNT 3**.

73. Discord, Inc. included the file in question, which the Provider had viewed, and your affiant subsequently viewed and verified. The JPG image file depicted a prepubescent female on her hands and knees displaying her unclothed vagina and anus. Included with the image was the .122 IP address, which was used to log into the account.

74. Discord, Inc. supplied the following subscriber information, associated with the user of **SUBJECT ACCOUNT 3**:

a. Email Address: **hardline2042@outlook.com** (Verified)
b. Screen/User Name: Vanhorn#1518
c. ESP User ID: 1049848180231127111
d. IP Address: **216.54.92.122** (Login) 12-12-2022 23:42:24 UTC

75. Therefore, based on this subscriber information, your affiant learned that **SUBJECT ACCOUNT 1** was a verified e-mail address associated with **SUBJECT ACCOUNT 3**, and the .122 IP address was used to upload a file to **SUBJECT ACCOUNT 3** on December 12, 2022.

76. On December 13, 2022, Discord, Inc. submitted a second CyberTip # 141478575 to the NCMEC regarding one of their users uploading child pornography to **SUBJECT ACCOUNT 3**.

77. Discord, Inc. included the file in question, which the Provider had viewed, and your affiant subsequently viewed and verified. The JPG image file depicted a prepubescent female performing oral sex on an adult male penis. Included with the image was the .122 IP address, which was used to log into the account.

78. Discord, Inc. supplied the following subscriber information, associated with the user of **SUBJECT ACCOUNT 3**.

Email Address: **hardline2042@outlook.com** (Verified)
Screen/User Name: Vanhorn#1518
ESP User ID: 1049848180231127111
IP Address: **216.54.92.122** (Login) 12-12-2022 23:42:24 UTC

79. This subscriber information reiterated that **SUBJECT ACCOUNT 1** was a verified e-mail address associated with **SUBJECT ACCOUNT 3**, and the .122 IP address was used to upload a file to **SUBJECT ACCOUNT 3** on December 12, 2022.

CONCLUSION

59. Based on the facts set forth above, I believe probable cause exists that the user(s) of the **SUBJECT ACCOUNTS** has violated the Target Offenses.

60. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachments B-1 and B-2) of such violations will be found within the **SUBJECT ACCOUNTS** (more precisely described in Attachments A-1 and A-2).

61. Accordingly, I request that a warrant be issued authorizing your affiant, with assistance from additional NCIS agents and other law enforcement personnel, to search the **SUBJECT ACCOUNTS** described in Attachments A-1 and A-2, for the items specified in Attachments B-1 and B-2.

62. Because the warrant will be served on the Providers who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

FURTHER AFFIANT SAYETH NOT.

Lindsey Santos, Special Agent
Naval Criminal Investigative Service
Norfolk, VA

SUBSCRIBED and SWORN to before me on 20th day of March 2024.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information, wherever stored, associated with

a. **hardline2042@outlook.com**
b. **hardline2077@outlook.com**

wherever located, which is or was stored at the premises owned, maintained, controlled, or operated by Microsoft Corporation USA, a company headquartered at 1 Microsoft Way, Redmond, WA 98052 to include that information preserved by Microsoft Corporation USA pursuant to a request submitted by NCIS on March 8, 2024.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation USA

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Microsoft Corporation USA, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Microsoft Corporation USA, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft Corporation USA is required to disclose the following information to the government for each account or identifier listed in Attachment A-1, for the time period of April 1, 2022 to the present:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Microsoft usernames (past and current) and the date and time each username was active, all associated Microsoft accounts (including those linked by machine cookie), and all records or other information about connections with Microsoft, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between Microsoft Corporation USA and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata.

C. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Microsoft users, including but not limited to:

1. Interactions by other Microsoft users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account, and;

F. All location information, including location history, login activity, information geotags, and related metadata.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (certain activities relating to the distribution and receipt of child pornography), and Title 18 U.S.C. § 2252(a)(4)(B) possession of child pornography), including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

A. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

B. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

C. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and,

D. The identity of the person(s) who communicated with the account holder about matters relating to sharing, possession, viewing, manufacturing, and/or ~~disturbing~~ distributing child pornography including records that help reveal their whereabouts.

E. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

F. Any person knowingly distributing, receiving, producing, or possessing child pornography

G. Evidence of the times the accounts or identifiers listed on Attachment ~~A~~ A-1 was used;

H. Passwords and data security devices, and other access information that may be necessary to access the accounts or identifiers listed on Attachment ~~A~~ A-1 and other associated accounts; and

I. Device backups including camera roll and photo stream data to identify child pornography, victims or contraband.

III. Method of Service/Delivery: Notwithstanding 18 U.S.C. § 2251 *et seq.* or similar statute or code, Microsoft Corporation USA shall disclose responsive data, if any, within fourteen days of service of the warrant, by sending it to Naval Criminal Investigative Service Special Agent Lindsey Santos, at NCIS Field Office Norfolk, VA, located at 1329 Bellinger Blvd., Norfolk, VA 23511. Items to be delivered to the government pursuant to this search warrant may be sent on any digital media device.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information, wherever stored, associated with the Discord, Inc. accounts:

a. Email Address: hardline2042@outlook.com
Screen/User Name: Vanhorn#1518
ESP User ID: 1049848180231127111

b. Email Address: hardline2077@outlook.com
Screen/User Name: Cassidy Harding#5154
ESP User ID: 1038972467848421376

c. Screen/User Name: Deleted User 4dc07823#7222
ESP User ID: 850446314859921451

wherever located, which is or was stored at the premises owned, maintained, controlled, or operated by Discord, Inc., a company headquartered at 444 De Haro St., Suite 200, San Francisco, CA 94107, to include information preserved by Discord, Inc., pursuant to a request submitted by NCIS on March 8, 2024.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Discord, Inc.,

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Discord, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Discord, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Discord, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A-2 from the time period of April 1, 2022 to the present:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Discord, Inc. usernames (past and current) and the date and time each username was active, all associated Discord, Inc. accounts (including those linked by machine cookie), and all records or other information about connections with Discord, Inc., third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, ~~October 3~~, April 1, 2022 until present;

7. Privacy and account settings, including change history; and

8. Communications between Discord, Inc. and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata.

C. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Discord, Inc. users, including but not limited to:

1. Interactions by other Discord, Inc. users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account and;

F. All location information, including location history, login activity, information geotags, and related metadata.

II. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (certain activities relating to the distribution and receipt of child pornography), and Title 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), including, for each account or identifier listed on Attachment A-2, information pertaining to the following matters:

A. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

B. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

C. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and,

D. The identity of the person(s) who communicated with the account holder about matters relating to sharing, possession, viewing, manufacturing, and/or disturbing child pornography including records that help reveal their whereabouts.

E. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

F. Any person knowingly distributing, receiving, producing, or possessing child pornography

G. Evidence of the times the accounts or identifiers listed on Attachment A was used;

H. Passwords and data security devices, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts; and

I. Device backups including camera roll and photo stream data to identify child pornography, victims or contraband.

III. Disclosure by provider - By Order of the Court

1. Notwithstanding 18 U.S.C. § 2251 *et seq*. or similar statute or code, Discord, Inc. shall disclose responsive data, if any, within fourteen days of service of the warrant, by sending it to Naval Criminal Investigative Service Special Agent Lindsey Santos, at NCIS Field Office Norfolk, VA, located at 1329 Bellinger Blvd., Norfolk, VA 23511. Items to be delivered to the government pursuant to this search warrant may be sent on any digital media device.